BAB I

PENDAHULUAN

1. Latar Belakang

Didalam masyarakat global saat ini Teknologi Informasi dan Komunikasi (TIK) merupakan suatu hal yang digunakan oleh masyarakat dalam mempermudah mereka melakukan aktifitas sehari.-hari.Salah satu produk teknologi yang saat ini digunakan untuk menguasai serta membantu hampir dari seluruh aspek kehidupan masyarakat pada umumnya adalah internet. Internet adalah 'jaringan dari seluruh jaringan' yang terdiri dari jutaan jaringan yang lebih kecil milik domestik, akademi, bisnis, pemerintahan, militer, non pemerintahan, yang secara bersama-sama membawa berbagai informasi dan pelayanan, seperti surat elektronik (email), online chat, pengiriman file, dan halaman–halaman *web* yang saling terhubung serta sumber lain dari *world wide web* (*www*).[1]Tidak heran karena adanya jaringan yang mencakup seluruh kalangan, internet digunakan baik oleh pelaku bisnis, pejabat, pemerintah ataupun masyarakat biasa baik dalam skala nasional maupun internasional untuk melakukan bisnis maupun hanya sekedar melakukan aktifitas dalam kehidupan sehari-hari.

Melalui Internet pertukaran informasi juga dapat dilakukan dengan cepat, mudah, dan biaya murah, ini dikarenakan internet tidak mempunyai batas (*borderless)* yang dimana sebuah informasi dapat melintasi antar suatu wilayah ke wilayah lainnya hanya dengan sekejap saja.Seiring dengan semakin populernya Internet sebagai "*The Network of the*

[1] Petrus Reinhard Golose, *Seputar Kejahatan Hacking Teori dan Studi Kasus,* Yayasan Pengembangan Kajian Ilmu Kepolisian (YPKIK), Jakarta, 2008, h. 7

Network", masyarakat penggunanya (*Internet Global Community)* seakan-akan mendapati suatu dunia baru yang dinamakan *cyber space* yang merupakan khayalan tentang adanya alam lain pada saat teknologi telekomunikasi dan informatika bertemu.

Kemajuan teknologi yang merupakan hasil budaya manusia disamping membawa dampak positif, dalam arti dapat digunakan untuk kepentingan umat manusia juga dapat membawa dampak negatif terhadap perkembangan kejahatan. Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet, kejahatan ini dalam istilah asing disebut dengan *cyber crime*.

Cyber crime berbeda dengan kejahatan tradisional pada umumnya, adapun beberapa perbedaan yang sangat mencolok antara *cyber crime* dengan kejahatan tradisional karena *cyber crime* atau kejahatan komputer dapat dilakukan secara anonim dan anonimitas merupakan cirinya yang utama, kejahatan komputer dapat pula mengakibatkan kerugian finansial yang luar biasa banyaknya dibandingkan kejahatan tradisional pada umumnya, serta kejahatan komputer dapat dilakukan dari tempat yang tidak dapat dideteksi oleh penegak hukum.

Cyber crime sebenarnya secara umum merupakan bentuk kejahatan biasa, hanya saja mengalami perkembangan dengan menggunakan teknologi. Menurut Dikdik M. Arief Mansur dan Elisatris Gultom jenis-jenis kejahatan yang termasuk *Cyber crime* dapat dikategorikan sebagai berikut: *cyber*–terorisme, *cyber*–pornography, *cyber*-harrasment, *cyber*–*stalking*, *cracking*, *carding*.[2]

Perkembangan *cyber crime* di Indonesia telah meningkat secara signifikan sejak 1998 seiring dengan meningkatnya pengguna internet di Indonesia saat itu telah mencapai 512.000 orang. Apalagi data terakhir

[2] Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi* , PT. Refika Aditama, Bandung, 2005, h. 26

menyebutkan Indonesia menempati urutan nomor dua tertinggi dalam penyalahgunaan kartu kredit.[3]

Adapun kejahatan *cyber crime* jenis baru yang cukup meresahkan banyak pihak adalah *phising* atau penipuan lewat *e-mail*. *Phising* merupakan teknik untuk mencari *personal information* (alamat *e-mail*, nomor rekening dan data pribadi lainnya) dengan mengirimkan *e-mail* yang seolah–olah datang dari bank yang bersangkutan.[4]

Dalam penulisan skripsi ini jenis kejahatan dunia maya (*cybercrime*) yang akan dibahas secara terperinci adalah pembobolan website (*deface*). Pembobolan website ialah suatu kejahatan jenis baru dalam ruang lingkup hukum pidana dan masih termasuk dalam jenis kejahatan dunia maya (*cybercrime*).Adapun jenis kejahatan pembobolan website yang sering kita lihat fenomenanya akhir–akhir ini adalah *hacking* dan *cracking*, pelaku yang melakukan hal tersebut disebut dengan *hacker* dan *cracker*.

Banyak kasus *cracking* yang terjadi di Indonesia misalnya peretasan *website* Komisi Pemilihan Umum, peretasan *website* milik partai Golkar, dan baru – baru ini pada tahun 2013 telah terjadi peretasan *website* pribadi milik Presiden Republik Indonesia Susilo Bambang Yudhoyono yaitu http://presidensby.info yang dilakukan oleh pemuda asal Jember bernama Wildan Yani Ashari.

Setelah melalui proses penyidikan lebih lanjut, terdakwa Wildan Yani Ashari ditangkap di warnet tempat dia bekerja yaitu Warnet Surya Com, Wildan melakukan peretasan terhadap website http://presidensby.info dengan cara terlebih dahulu melakukan akses ilegal

[3] H. Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, PT. Refika Aditama, Bandung, 2005, h. 130 dikutip dari Arief Pitoyo, *Bisnis Indonesia*, 2004

[4] *Ibid*, h. 132

kedalam *web hosting* http://techspace.co.id yang kemudian dalam pengaksesan hal tersebut ditemukan DNS Server dari domain http://presidensby.info sehingga terdakwa dapat mengakses *website* milik presiden Susilo Bambang Yudhoyono tersebut.

Website http://presidensby.info kemudian setelah diretas oleh terdakwa berubah tampilan *website*nya menjadi hitam dengan lambang tengkorak bertuliskan Jember Hacker Team, sehingga terdakwa didakwa dengan pasal 46 ayat (1) jo. pasal 30 ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan pasal 406 KUHP ayat (1) yang bunyinya:

> "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak RP 1.000.000.000,00 (satu miliar rupiah)."[5]
>
> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun."[6]
>
> "Barangsiapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak tiga ratus rupiah."[7]

---

[5] Pasal 46 Ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)

[6] Pasal 30 Ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)

[7] Pasal 406 Ayat (1) KUHP

Berdasarkan latar belakang di atas maka penulis merumuskan dalam judul ***Pertanggungjawaban Pidana CRACKER yang melakukan Peretasan Website Presiden Ditinjau dari Undang-Undang No. 11 Tahun 2008 tentang INFORMASI DAN TRANSAKSI ELEKTRONIK (Studi Kasus Putusan No. 253/Pid.B/2013/PN JR).***

2. Perumusan Masalah

a. Bagaimana unsur–unsur pengaturan *cracking* menurut UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan UU No. 36 tahun 1999 tentang Telekomunikasi?

b. Bagaimana Pertanggungjawaban pidana Pelaku Tindak Pidana dalam kasus peretasan website?

3. Ruang Lingkup Penulisan

Sesuai permasalahan di atas, maka ruang lingkup penelitian dibatasi pada unsur-unsur pertanggungjawaban pidana*cracker* dan pertanggungjawaban pelaku tindak pidana yang melakukan peretasan terhadap *website* pribadi milik presiden SBY dengan No. perkara 253/Pid.B/2013/PN JR.

4. Tujuan dan Manfaat Penelitian

a. Tujuan Penelitian

Adapun tujuan dari penulisan skripsi ini adalah:

1) Untuk mengetahui unsur – unsur pengaturan *cracking* didalam UU ITE dan KUHP.
2) Untuk mengetahui bentuk pertanggungjawaban pidana pelaku tindak pidana *cyber crime* dalam kasus peretasan *website* milik pribadi.

b. Manfaat Penelitian

Selanjutnya penulisan skripsi ini juga di harapkan bermanfaat untuk

1) Secara teoritis, hasil penelitian ini penulis harapkan dapat bermanfaat bagi penulis, rekan–rekan sesama pelajar maupun para penegak hukum sebagai referensi.
2) Secara praktis, dapat mengetahui dan memahami kepastian hukum dari penyelesaian kasus tindak pidana *cyber crime*.

5. Kerangka Teori dan Kerangka Konseptual

a. Kerangka Teori

Teori Pertanggungjawaban Pidana

Pada waktu membicarakan pengertian perbuatan pidana, telah diajukan bahwa dalam istilah tersebut tidak termasuk pertanggungan jawab. Perbuatan pidana hanya menunjuk kepada dilarang dan diancamnya perbuatan dengan suatu pidana. Apakah orang yang melakukan perbuatan kemudian juga dijatuhi pidana, sebagaimana telah diancamkan, ini tergantung dari soal apakah dalam melakukan perbuatan ini dia mempunyai kesalahan.[8]

Bahwa adanya kelakuan yang melawan hukum, itu belum cukup menjatuhkan hukuman, sebab harus ada seorang (atau lebih) pembuat (*dader*) yang bertanggung jawab atas kelakuannya. Umumnya dapat diterima pendapat bahwa untuk adanya suatu peristiwa pidana harus ada dua anasir yang dipenuhi yaitu:

1) Suatu kelakuan yang melawan hukum (anasir melawan hukum)
2) Seorang pembuat yang dapat bertanggung jawab atas kelakuannya.

Juga umumnya diterima pendapat bahwa hukum positif berpegang pada azas : “Tiada hukuman tanpa kesalahan” (*Geen straf zonder*

[8] Moeljatno, *Azas-Azas Hukum Pidana*, Bina Aksara, Jakarta, 1987, h. 104

schuld).[9] Azas ini tidak tersebut dalam hukum tertulis tapi dalam hukum yang tidak tertulis juga di Indonesia berlaku. Hukum pidana fiscal tidak memakai kesalahan. Disana kalau orang telah melanggar ketentuan, dia diberi pidana denda atau rampas.[10]

Menurut para sarjana hukum, bahwa untuk adanya kemampuan bertanggung-jawab harus ada:

a) Kemampuan untuk membeda-bedakan antara perbuatan yang baik dan yang buruk; yang sesuai hukum dan yang melawan hukum;
b) Kemampuan untuk menentukan kehendaknya menurut keinsyafan tentang baik dan buruknya perbuatan tadi.[11]

Kemampuan bertanggung-jawab merupakan unsur (elemen) kesalahan. Karenanya mestinya untuk membuktikan adanya kesalahan, unsur tadi harus dibuktikan pula. Ini sangat sukar, lagipula memakan banyak waktu dan ongkos. Oleh sebab itu, karena pada umumnya orang-orang adalah normal batinnya, dan mampu bertanggung-jawab, maka unsur ini dianggap diam-diam selalu ada, kecuali kalau ada tanda-tanda yang menunjukkan bahwa terdakwa mungkin jiwanya tidak normal.[12]

Dalam pertanggungjawaban pidana terdapat doktrin *mens rea* yang disebut-sebut sebagai dasar dari hukum pidana, kata "*mens rea*" ini diambil orang dari suatu maxim yang berbunyi: *actus non est reus nisi mens sit rea*, yang maksudnya adalah suatu perbuatan tidak menjadikan seseorang bersalah kecuali pikirannya adalah salah. Dan

[9] R. Atang Ranoemihardja, *Hukum Pidana Azas – Azas, Pokok Pengertian dan Teori serta Pendapat beberapa Sarjana*, Tarsito, Bandung, 1984, h. 43-44

[10] Moeljatno, *loc. Cit.*

[11] *Ibid,* h. 112

[12] *Ibid,* h. 113-114

yang dimaksud dengan pikiran salah tentunya adalah pikiran jelek. Ada yang mengatakan bahwa rumusan seperti dikemukakan diatas mungkin sekali adalah pernyataan yang tidak teliti dari suatu prinsip yang sebenarnya adalah lain, yaitu bahwa *mens rea* adalah suatu kehendak untuk melakukan suatu perbuatan yang adalah salah dalam arti dilarang oleh Undang-Undang.[13]

b. Kerangka Konseptual

1) Pertanggungjawaban pidana

Suatu perbuatan yang tercela oleh masyarakat yang harus dipertanggungjawabkan pada si pembuatnya atas perbuatan yang dilakukan.[14]

2) *Cracker*

Manusia yang menggunakan internet dengan tujuan jahat yang membuat pemakai internet tidak nyaman.[15]

3) *Website*

Keseluruhan halaman-halaman *web* yang terdapat dalam sebuah domain yang mengandung informasi.[16]

6. Metode Penelitian

[13] Roeslan Saleh, *Pikiran-pikiran Tentang Pertanggungjawaban Pidana*. Ghalia Indonesia, Jakarta, 1982, h. 21-23

[14]*Ibid*, h. 75-76

[15] Agus Raharjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, 2002, h. 132

[16]Hidayat, Rahmat, *Cara Praktis Membangun Website Gratis*. Jakarta: PT Elex Media Komputindo. 2010, h. 2

a. Jenis Penelitian

Metode yang digunakan dalam penelitian ini adalah penelitian hukum normatif atau kepustakaan yang menekankan terhadap literature hukum perdata dan perundang-undangan yang berlaku.Penelitian hukum normatif adalah metode penelitian hukum yang dilakukan dengan meneliti bahan pustaka atau data sekunder berkala.

b. Pendekatan Masalah

Di dalam penelitian hukum terdapat beberapa pendeketan. Dengan pendekatan tersebut, peneliti akan mendapatkan informasi dari berbagai aspek mengenai isu yang sedang dicoba untuk mencari jawabannya.

1) Pendekatan perundang-undangan :
   a) Kitab Undang-Undang Hukum Pidana
   b) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;
   c) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
2) Pendekatan Kasus

Dalam skripsi ini menggunakan Putusan Negeri Jember Nomor 253/PID.B/2013/PN JR.

3) Pendekatan Konseptual

Pada penelitian ini penulis menemukan beberapa definisi-definisi berdasarkan undang-undang dan pendapat para ahli yang berkaitan dengan judul skripsi ini.

c. Sumber Data

Sumber data yang digunakan dalam penelitian hukum normatif adalah data sekunder, yang terdiri dari 3 sumber bahan hukum:

1) Sumber Bahan Hukum Primer

Sumber Bahan Hukum Primer yaitu bahan hukum yang terdiri atas peraturan perundang-undangan secara hierarki dan putusan-putusan pengadilan.

2) Sumber Bahan Hukum Sekunder

Sumber Bahan Hukum Sekunder yaitu bahan hukum yang terdiri dari buku teks, jurnal hukum, pendapat para pakar, yurisprudensi, hasil penelitian, dan lain-lain bahan hukum diluar dari bahan hukum primer.

3) Sumber Bahan Hukum Tersier

Sumber Bahan Hukum Tersier yaitu bahan hukum yang diperoleh dari kamus hukum atau ensiklopedia yang berkaitan dengan bidang hukum.

d. Teknik Analisis Data

Teknik Analisis Data, merupakan langkah-langkah yang berkaitan dengan pengolahan terhadap bahan-bahan hukum yang telah dikumpulkan untuk menjawab rumusan masalah yang dilakukan dengan cara analisis kualitatif. Sedangkan untuk menganalisa bahan hukum digunakan teknik penulisan Deskriptif Analisis, yaitu menjelaskan secara rinci dan sistematis terhadap pemecahan masalah.

7. Sistematika Penulisan

Untuk memudahkan dan memberikan gambaran aka nisi penulisan skripsi ini, maka disusun sistematika penulisan yang terdiri atas 5 (lima) bab, yaitu :

BAB I PENDAHULUAN

Dalam bab ini menguraikan tentang latar belakang, perumusan masalah, ruang lingkup penulisan, tujuan dan manfaat penelitian, kerangka teori dan kerangka konseptual, metode penelitian dan sistematika penulisan.

BAB II TINJAUAN UMUM TENTANG TINDAK PIDANA *CYBER CRIME* DAN *CRACKING*

Bab ini menjelaskan tinjauan umum tentang tindak pidana, tindak pidana *cyber crime*dan tindak pidana *cracking* serta pertanggungjawaban pidana pelaku tindak pidana *cyber*

crime dan pengertian *cracking* didalam pengaturan UU No. 11 Tahun 2008 tentang Informasi dan Teknologi Elektronik

BAB III PERTANGGUNGJAWABAN PIDANA CRACKER DALAM KASUS CRACKING WEBSITE PRIBADI PRESIDEN SBY (STUDI KASUS PUTUSAN NO. 253/PID.B/2013/PN JR)

Bab ini menjelaskan kasus posisi, surat dakwaan, keterangan jaksa, tuntutan jaksa, penuntut umum, pertimbangan hakim dan analisis atas putusan Pengadilan Negeri Jember.

BAB IV ANALISA YURIDIS TERHADAP PENGATURAN CRACKING DALAM UU ITE DAN KUHP DAN PERTANGGUNGJAWABAN PIDANA PELAKU DALAM TINDAK PIDANA PERETASAN WEBSITE PRIBADI MILIK PRESIDEN SBY

Bab ini menguraikan analisis tentang bagaimana unsur-unsur pengaturan *cracking* didalam UU ITE dan KUHP dan pertanggungjawaban *cracker* yang melakukan peretasan *website* pribadi milik presiden SBY yang dilakukan oleh Wildan Yani Ashari.

BAB V PENUTUP

Bab ini merupakan bagian akhir dari penulisan, penulis berusaha menyimpulkan dari bab terdahulu mengenai rumusan masalah yang kemudian penulis mencoba untuk memberikan saran-saran yang kiranya dapat dijadikan masukan bagi berbagai pihak yang berkepentingan